8 April 1993 Final Student Research Report

C4I For The Warrior: Will This Dog Hunt?

Captain C. R. Bigger, USA; Captain D. L. Robbins, USMC; Captain E. J. Ryan, USAF; Captain A. R. Mellon, USMC

Command and Control Systems Course
Communication Officer's School
2085 Morrell Avenue
Quantico, Virginia 22134-5058

Marine Corps University
Marine Corps Combat Development Command
2076 South Street
Quantico, Virginia 22134-5068

Thesis: Successful implementation of C4I For The Warrior (C4IFTW) is dependent upon overcoming technical issues, budgetary constraints, and lack of cooperation between the armed services. This paper examines past, present and future technologies involved with the C4IFTW concept.

USMC; Command and Control; C2; C3; C4I; Joint Command and Control; C4IFTW; JITC; CIM; DISA; Defense ADP; Data Standards; Interoperability 29

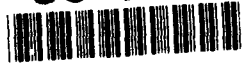
Unclassified Unclassified Unclassified

C4I FOR THE WARRIOR: WILL THIS DOG HUNT?

Submitted to
Major M.K. Snyder
and Mrs. Sandra Kirkpatrick
at the Communication Officers School
Quantico, Virginia

Captain C.R. Bigger, USA
Captain D.L. Robbins, USMC
Captain E.J. Ryan, USAF
Captain A. R. Mellon, USMC

8 April 1993



C4IFTW: WILL THIS DOG HUNT?

OUTLINE

Thesis statement: Successful implementation of C4IFTW is dependent upon overcoming technical issues, budgetary constraints, and lack of cooperation between the armed services.

I. Introduction. The time is right.
   A. Past operations.
   B. Advancing technologies.
   C. Changing Military Strategy.

II. C4IFTW overview.

III. Starting the C4IFTW campaign.
   A. Selling the concept.
   B. The advertising campaign.

IV. The doctrine and policy battle.
   A. DoD Directive 4630.5.
   B. DoD Instruction 4630.8.

V. The first big step: Translators.
   A. Limiting the formats.
   B. Prototypes and demonstrations.

VI. The multi-level security hurdle.
   A. Political problems.
   B. MLS Technology Insertion Program.
   C. Testbeds.
   D. Marine Corps MLS efforts.

VII. The first large scale test: C4IFT(P)W.

VIII. A systematic approach to establishing joint standards
   A. DISA creation/responsibilities.
   B. Standards with flexibility.
   C. Suggested approaches.

IX. The Joint Interoperability Test Center (JITC).
   A. JITC's authority and responsibilities.
   B. JITC's capabilities.

X. Effects of Corporate Information Management Initiative.
   A. Purpose of CIM.
   B. Implementation of CIM.

XI. Conclusion.

Appendix A - 13 Standard Data Formats

C4I FOR THE WARRIOR: WILL THIS DOG HUNT?

INTRODUCTION TO C4I FOR THE WARRIOR

The time is right for an interoperable Command, Control, Communications, Computers, and Information (C4I) system. Recent world events have shown that the C4I systems in the U.S. Armed Forces are not interoperable and that interoperability is a necessity in future operations. Operations Urgent Fury, Just Cause, and Desert Storm identified difficulties that the services experienced in exchanging information. This problem is receiving great attention now that national military strategy is focused on joint and combined operations in regional conflicts rather than on the Soviet Threat. In response to the need for interoperable command and control systems, the Joint Chiefs of Staff, J-6 developed a concept called C4I for the Warrior (C4IFTW). C4IFTW is a global C4I systems infrastructure providing joint interoperability among services for information flow at all echelons. Successful implementation of C4IFTW is dependent upon overcoming technical issues, budgetary constraints, and lack of cooperation between the armed services.

C4IFTW OVERVIEW

The concept, created in response to the recognized need for interoperable systems, is technologically possible based

upon recent advancements in automation and telecommunications. C4IFTW is an evolutionary concept with three phases that will maximize current C4I systems and control future acquisition of C4I systems through the enforcement of interoperability standards. In time, the concept calls for a fully interoperable system which makes battlefield information readily accessible to all combat commanders.

The proposed DoD Directive for "C4I for the Warrior" dated 6 April 1992 provides a concept statement for C4IFTW. It defines the three phases of the concept, and outlines agency and service responsibilities. This directive calls for the warrior (defined as a combat commander at any echelon) to have the ability to plug-in anytime, anywhere, into a global infrastructure which interconnects a number of fusion centers with national databases.

The three phases of C4IFTW are the Quick Fix Phase, Midterm Phase, and the Final or Objective Phase. The Quick Fix Phase is a band-aid remedy to get the services exchanging information quickly using current C4I systems. We will develop a common set of data formats, use translators to merge data systems with different protocols, and enforce interoperability standards during acquisition of new systems. The Midterm Phase, approximately ten years out, will develop the global infrastructure. This infrastructure will use fixed and mobile communications

centers and multi-functional switches as pipelines for all transmission media. This network of fused national databases will be accessible to any warrior. During the Objective or Final Phase, which extends past the year 2000, a fully developed global infrastructure of interconnected automatically updated national databases will be constructed. Warriors and the databases will be connected through national, international, and military telecommunications systems.

STARTING THE C4IFTW CAMPAIGN

In 1991 Gen. Powell, Chairman of the Joint Chiefs of Staff, told Adm Macke, the Joint Staff J-6, to find out why the Marines and the Army had trouble communicating tactically during the Persian Gulf War and to solve the problem. The C4IFTW concept was the result of that conversation.(7) Selling the concept to a skeptical market in the services and the DoD agencies was tough. Service and DoD agency officials have seen previously proposed command and control systems which were touted as the solutions to our interoperability problems. Programs like Tri-Tac produced limited interoperability results and caused conflicts between services and agencies competing for defense dollars. Other concepts have fallen by the wayside once leading supporters have moved on or retired. The fact that C4IFTW is not threat driven (i.e. developed

If their standards are found feasible to the C4IFTW cause,

specifically to counter an enemy capability) and the successful outward appearance of the Desert Storm C2 may lead some to believe this initiative is not necessary. Additionally, the concept was not originated by the "operators" and is not as tangible as a new artillery piece. The J-6 staff needed a strategy to get the concept accepted and into the individual service/agency/CinC agendas.(7)

The services, past and present, continue to work on their own solutions to the C2 problem, with each service developing systems of its own. Rather than starting from scratch with a new comprehensive system, the C4IFTW concept looks to ensure that the service developed systems will be interoperable and complimentary.(7) Unifying all of these efforts and individual interests and selling them to the market took advertising.(7) The approach used to sell C4IFTW concept is a significant part of the concept itself. Getting the services and agencies on the bandwagon of interoperability is the only way the problem will be solved.

In 1991 Adm Macke, with Col Bryan of the J-6 office, developed a brief to deliver to the Joint Chiefs and the brief has expanded dramatically since then.(7) The "advertising campaign" contributed to the development of the C4IFTW concept, as simple ways of expressing complex problems were refined. Brochures were developed in house using contractors for graphics and printing. Over 12,000 have been distributed. Video brochures, including a 90

warrior's requirements will surely change throughout the

minute presentation, were produced with professional assistance. "Tiger Teams" were established and dispatched to the CinC's to provide briefs and solicit comments. Groups ranging from Congress to the American Petroleum Association have received C4IFTW presentations. The J-6 staff has attempted to sell and institutionalize the C4IFTW concept at all levels.(7) Although some may see the advertising effort as time and money taken away from actual concept development, the effort was a necessary expense and should continue in order to cultivate C4IFTW followers. Only if senior service members are convinced of its viability will the concept survive.

Advertising does little without concrete product performance to back it up, and the J-6 staff has put a great deal of effort into making real progress toward the concept's implementation. They proudly point to long list of "trophies," or accomplishments, to show the concept's approach is working. Some of these trophies, such as establishment of doctrine and policy, and the development of translators will examined throughout this paper.

THE DOCTRINE AND POLICY BATTLE

A tangible step toward institutionalizing C4IFTW is Department of Defense (DoD) Directive, Number 4630.5, SUBJECT: Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I)

Systems, dated November 12, 1992. This precedent-setting policy directs integration of C3I systems and assigns responsibilities to the CJCS and armed services during development and acquisition of new C3I systems and equipment.

The policy directs that forces involved in joint or combined operations must be supported by an integrated C3I system that is interoperable. It calls for services to develop and acquire interoperable systems that meet essential operational needs of U.S. Armed Forces. In line with the direction of C4IFTW's Objective Phase, paragraph D.4 of the directive states, "For the purposes of compatibility, interoperability, and integration, all C3I systems developed for use by U.S. Armed Forces are considered to be for joint use."

DoD Directive 4630.5 and DoD Instruction 4630.8 establishes responsibilities for compliance with the directives. Most notably the Chairman of the Joint Chiefs of Staff is directed to establish procedures for development and validation of compatibility. The CJCS is also responsible for approving, documenting and exercising doctrinal concepts. The Defense Information Systems Agency (DISA) will test and evaluate C3I systems. It will administer compatibility, interoperability, and intcgration certification tests and certify to the CJCS that the C3I system operate within a joint interface.

DoD Directive 4630.5 and DoD Instruction 4630.8 set a precedent by placing a higher level of control over the services in their acquisition of C3I systems. The necessary testing and review are required prior to funding, thus strong arming the services into compliance. The actual effectiveness of the instruction will, of course, depend on how strictly the Joint Staff and DISA enforce the instruction's intent.

THE FIRST BIG STEP: TRANSLATORS/INTERPRETERS

A major tool in the near-term, quick-fix phase is the interpreter (or translator). An interpreter is a special software program that takes the language that one command and control system speaks and translates it into language that another command and control system can understand. A fully integrated set of interpreters would enable almost all of the U.S. military's command and control systems to share information. Such a solution, though, is complicated by the more than 50 major command and control systems operated by today's U.S. military.(5)

To build an interpreter, the J-6 C4IFTW Interoperability Tiger Team first set out to define a set of data format standards. After studying existing systems and data format standards, the Tiger Team devised a set of 13 formats (see Appendix A) which will provide basic interoperability between the existing systems.(5) The Tiger

Team then took this set of data formats to the CINCs to solicit their suggestions and to further refine the formats.

With the data format standards in hand, the next step was to create a prototype interpreter and provide a proof of concept. On 20 November 92, the Naval Electronic Systems Engineering Activity (NESEA) demonstrated the initial prototype interpreter, the Joint Universal Data Interpreter (JUDI).(2) This first version of JUDI provided a limited interface capability between the Army's Standard Theater Army Command and Control System (STACCS) and the Navy's Joint Operational Tactical System (JOTS).(2) In March 1993, NESEA demonstrated a fully integrated capability between these two systems, and, on 7 April 1993, NESEA showed an integrated capability between JOTS, STACCS, the Marine Corps' Intelligence Analysis System (IAS), and the U.S. Air Force's Air Situation Display System (ASDS).

The next step is to install the JUDI prototype into European Command (EUCOM) for use as an operational testbed. Initial interoperability tests with the USCINCEUR Command Center System (UCCS) have been completed. In April 1993, the fully integrated JUDI prototype is scheduled to demonstrate its capabilities within EUCOM.(2)

The U.S. Air Force's Contingency TACS Automated Planning System (CTAPS) will be the next command and control system to be integrated. The demonstration of this capability is scheduled for May 1993.(2) Continued

interpreter/translator development, vital to the Quick-Fix Phase of the C4IFTW program, is ahead of schedule. Current advances are bringing the first phase of the C4IFTW program much closer to successful completion. As work on interpreters continues, DISA, the CINCS, and the individual Services are collectively working to pare down many of the superfluous command and control systems currently in existence. Continued integration, and, if necessary, elimination, of U.S. military command and control systems in the Quick-Fix phase will give future C4IFTW efforts a solid foundation on which to build. However, failure to meet the near-term goals could mark C4IFTW as another fly-by-night proposal and potentially eliminate much needed support.

THE MULTI-LEVEL SECURITY HURDLE

One technological obstacle which must be overcome for the C4IFTW "global infrastructure" concept to work is the multi-level security (MLS) issue. Currently, data networks dealing with various levels of classified information are kept separate, requiring redundant computers, servers, and transmission paths for each. C4IFTW envisions a single network which can be used for all levels of classified information and yet retain the ability to closely control access to each level. "MLS may be a show stopper," says one senior JCS officer.(7)

The problems appear to be both political and technical, according to experts on the DoD MLS problem.(15) The National Security Agency (NSA) is responsible for setting the standards for DoD computer security. The rules and guidelines for establishing multi-level security systems are defined in the Trusted Computer System Evaluation Criteria issued by the NSA.(14) These guidelines, and the NSA, have been criticized for their inflexibility when applied to the tactical level of DoD data networks. By applying the same rigorous standards to tactical systems which are applied to strategic systems, NSA creates a potential seven-year technology gap. (15) In the NSA's defense, its penchant for not trusting people or software, only hardware, to solve the MLS problem is grounded in the long history of security apathy in the DoD computer user community. NSA points out that in the future all tactical systems will be linked to strategic systems, requiring the same protection.

The MLS Technology Insertion Program (MLSTIP) was established to coordinate the efforts of the various interested DoD parties. The program's functions to are oversee and coordinate the use of resources, to establish efficient testbeds, and to develop plans and architectures.(19)

Currently, when using data networks (separated by classification), transferring large files such as Oplans can take up to six hours.(18) The envisioned systems will link

the variously classified networks and have "trusted" hardware at the connections to insure only authorized information is shared. One DoD expert describes the system as one big pipe with many smaller ones inside and valves to control the flow and interconnectivity at various intervals.(15)

In February 1993, the Defense-Wide Information Security System Program (DISSP) unveiled an architecture plan to make this concept a reality. Other MLS related programs must align within this architecture in long term applications. (18)

The core requirements to make the MLS program work are:

-Secure system interface.

-Secure networks.

-Secure multi-level workstations.

-Secure reclassification (downgrading).

-integrations of secure components, to include: guards, workstations, LAN, and host architectures.

-Secure shared data base (the longest-term problem). (18)

Many MLS advances have already been achieved. The testbed established by the MLSTIP has been very successful in creating working models at the U.S. Transportation Command (TRANSCOM) and the U.S. Central Command (CENTCOM). At TRANSCOM, the Air Mobility Command Global Decision Support System now has linked a top secret network with a

secret network using a trusted guard.(18) Tiger Teams have visited all Unified Commands and are addressing similar requirements with surprising speed. Many of the CinCs will have trusted systems on line in the next few months. In 1994 a multi-level electronic mail system is expected to be in place and MLS workstations will be introduced.(18)

The services are also very involved in the MLS development process. Each service has a program pertaining to its MLS needs. The Marine Corps will continue to separate tactical data networks of differing classification, but anticipates combining some networks by 1995. It is examining connecting tactical and strategic networks with a trusted interface called a Logical Coprocessing Key (LOCK). Additionally the Marine Corps is working with the SAIC corporation to develop a near term MLS system for use at the Marine Expeditionary Force (MEF) and MEF Forward (MEF FWD) level.(14)

While the MLS problem is perhaps the most technology driven hurdle in the C4IFTW concept, it is solvable. In fact, recent predictions of full implementation in 2000 may be conservative with the rate of technology development today.(19) The key to this technological solution will be money. Whether or not the DoD and the services will continue to put money into MLS development will be determined by the upcoming budget cuts and the priority placed on developing the C4IFTW concept. The responsibility

for prioritization will lie with the individual services.

THE FIRST LARGE SCALE TEST: C4I FOR THE PACIFIC WARRIOR (C4IFT(P)W)

C4IFT(P)W is the prototype program that will prove, on a large scale, the concepts and technologies of the C4IFTW vision. The United States Pacific Command's (USPACOM) vast area of responsibility presents a great communications challenge for CINCPAC. However, this challenge also provides an excellent arena for testing interoperability concepts.

USPACOM has already taken the lead in integrating its command and control systems by making the Operations Support System (OSS) its common CINC command and control system. The OSS is a program that integrates the following sub-systems on a LAN: the Operational Support Group Prototype (OSGP), the Joint Operational Tactical System (JOTS), and the Fleet Command Center Battle Management Program (FCCBMP).(12) USPACOM is planning to install OSS terminals at all of its components, connecting them with a Wide Area Network (WAN).(12)

USPACOM has also taken the lead role in implementing the two tier Command and Control concept where the JTF commander reports directly to the CINC, versus the traditional three-tiered system of reporting via the service components. As a result, CINCPAC created the Enhanced

Crisis Management Capability (ECMC) group which contains a suite of JTF command and control equipment that can be rapidly deployed. This equipment is connected to other USPACOM command centers via the Officer in Tactical Command Information Exchange System (OTCIXS) to form the Joint Area Information System Pacific (JAISPAC). This system provides positional and narrative messages for the JTF.(12) Looking to the future, C4I For The Pacific Warrior has created a roadmap of execution options that, if funded, will further work to prove the value of the C4IFTW concepts.

A SYSTEMATIC APPROACH TO ESTABLISHING JOINT STANDARDS

C4IFTW will not become a reality by simply establishing the standards for the joint exchange of information. But identifying joint standards is a logical and feasible first step in the evolution of the ultimate system. Identifying joint standards, although an evolving process which influences all future systems, represents the swiftest and least costly path to provide joint interoperability in the short term, or Quick Fix Phase.

The current tactical information systems that exchange information through a joint architecture certainly do not meet all the requirements of the definition of what C4IFTW needs; however, they will establish a useful information base for a joint or combined theater of operations.

A major "trophy" for defining C4IFTW joint standards has been placed upon the J-6 shelf with the establishment of DoD Directives 4630.5 and 4630.8. These directives have institutionalized the Defense Information Systems Agency (DISA), along with its subordinate affiliate, the Joint Interoperability and Evaluation Organization (JIEO) as the DoD focal point for standards.(3)

By requiring all C3I systems developed for use by the U.S. Armed Forces to be considered to be for joint use and required to meet joint standards, these directives have provided the needed impetus for service subordination to DISA and JIEO. Now, services interested in C3I system development, procurement, or use must first ensure joint C3I system compatibility, interoperability, and integration before they can purchase the equipment.(3) The reality: no interoperability, no money.

Interoperability requires defining the criteria for exchanging information. A straight-forward definition of the joint standard for C4IFTW would meet this criteria. We must avoid the historical tendency to define the total system in too much detail. If an all encompassing set of standards is included in the definition, the C4IFTW's joint information exchange standard will drive costs well beyond budget constraints and prove to be impossible to meet. The program will eventually lose both popular support and, finally, financial backing. Numerous systems developed in

this fashion, though perhaps well intended, fill the information systems' grave yard.

Instead, a more flexible and realistic approach is needed to define the criteria for the joint exchange of information and will serve the purpose of realizing the Objective Phase. For, just as the method of war continues to evolve, the warrior's communication and information requirements also will evolve. By simply defining the data elements, data base, and communications protocol required to input and extract information in a joint environment, the ingrained flexibility and growth characteristics of this approach will support the warrior's changing requirements. These joint standards will then be sufficient to ensure information can be exchanged between machines and systems, regardless of service affiliation. Thus, the interfaces are the key elements that need to be identified in the joint interoperability standard.

A systematic approach to defining the C4IFTW joint interoperability standards must be established. This approach will not eliminate existing standards and systems, but on the contrary, focus initial effort on all current assets, systems, facilities, and industries available. MTF, TADIL, logistic data elements, and personnel systems' standards, just to name a few, would be an easy enough target for the up-front investigation in order to learn what is "salvageable" and applicable for C4IFTW joint standards.

If their standards are found feasible to the C4IFTW cause, the Defense Advance Research Project Activity (DARPA) would be commissioned to catalogue these existing standards across the board.

The next step to this systematic approach is to continuously look to the commercial industry for standards that apply to the C4IFTW effort. With shrinking DoD budgets a reality, maximum service use of commercial off-the-shelf (COTS) systems, technologies, and equipment will minimize, and may in time even eliminate, related DoD research and (R&D) costs. Taking full advantage of COTS advancements will therefore play an ever increasing roll in C4IFTW standards and technology, and help to ensure the success and longevity of C4IFTW. In addition, coordination with the ongoing efforts of the Corporate Information Management (CIM) initiatives will further facilitate C4IFTW planners the ability to keep abreast of the latest developments and availability of private industries' state of the art technologies. Maintaining close contact with private industries and establishing a working relationship with them will ensure optimal support to the warrior through an evolutionary and dynamic C4IFTW joint system.

The final step in this systematic approach is the requirement to remain both flexible and efficient when identifying elements which comprise the C4IFTW's joint standards. The approach must be flexible to change, for the

warrior's requirements will surely change throughout the evolution of C4IFTW. While meeting the warrior's requirements, the number of joint standards needs to be kept as lo. as possible.(3) Grouping information that has common use or definition into a few categories will be cost effective and facilitate joint operability testing.

JOINT INTEROPERABILITY TEST CENTER (JITC)

Just as C4IFTW will not be realized by merely establishing and promulgating the standards for the joint exchange of information, testing established joint standards with today's procedures is inadequate to ensure true joint interoperability and will also fail to contribute to C4IFTW's Objective phase realization. An unbiased facility with no affiliation to any one service or private industry had to be identified. This facility would conduct testing for compliance with the established and true joint interoperability standards and provide interoperability certification. The Joint Interoperability Test Center (JITC) at Fort Huachuca, Arizona, has been identified as the site to provide this critical support.(9)

JITC can provide the CINCs, services, agencies, and others a real world evaluation of C4IFTW standards at the degree of joint interoperability within the confines of their facility and through an eventual dial-in network.(3) JITC's charter for testing joint interoperability standards

will ensure that both new and modified systems, along with data formats vying for entry into the C4IFTW project meet all joint interoperability standards prior to funding.

With DODD 4630.5 and 4630.8 firmly established, the JITC participation in C4IFTW will play an integral part in the overall success of the testing and development of all C4IFTW joint standards and systems. Sensitive to current budgetary constraints, JITC's testing for interoperability throughout the C4IFTW process, as opposed to JITC's waiting on a production model from which to perform the interoperability testing, will permit cheaper modifications. Further, the dial-in testing network established by the JITC is extensive and growing. Tremendous cost savings will be realized through this network. Equipment (military or commercial) does not have to be sent to Fort Huachuca, Arizona. Instead, it can be subjected to JITC's interoperability testing through the dial-in testing network. This capability will enable testing in the early stages of development while maintaining the low cost benefit.

EFFECTS OF CORPORATE INFORMATION MANAGEMENT INITIATIVE

The Corporate Information Management (CIM) initiative, a management method commonly referred to in the private sector as Business Process Improvement (BPI), is now also used by DoD. Its purpose is to reduce Defense Management

Report (DMR) costs while maintaining or improving the effectiveness of military missions. It accomplishes these cost savings and stream-lined procedures by eliminating non-value-added work and, more importantly, by improving the management of information. As a result, CIM has played, and will continue to play, an important role in DoD by facilitating the adoption of more efficient business management practices to even tactical systems, including C4IFTW. CIM's positive impact on C4IFTW will focus on satisfying the warriors information requirements, progress to the Objective Phase by way of small steps, returning to basics, ensuring centralized policy direction, facilities, and system procurement, and finally, decentralized execution.(1) However, even with these far reaching benefits foreseen, inherent problems do exist.

Although the CIM Initiative has made progress through conceptual acceptance, its actual implementation by DoD has been criticized as slow and detrimental to the C4IFTW effort. This dragged foot, on the part of DoD, has resulted in lost benefits to the C4IFTW progress, not soon, if ever, to be recovered. Its reluctance to implement this initiative may be justified, for CIM is one of the largest information management initiatives ever undertaken. DoD's success in coming to terms with this management challenge is threatened by three interlocking problems--issues that center around whether DoD can change long-standing,

fundamental aspects of its culture and whether business processes or technology becomes the driving force in managing DoD information.(10)

First, all agencies (DoD, CINCs, and Armed Services) are attempting to redefine their roles and missions in an attempt to justify their existence and claim their fair share of the budgetary pie. DoD has not established formal policies or directives addressing how the respective roles of the military services and the Office of the Secretary of Defense (OSD) should change to meet CIM's goals, even though CIM requires that control over business operations be centralized. This lack of direction from DoD, although not completely detrimental to the C4IFTW effort and progress, has, to a certain degree, inhibited its subordinate agencies' ability to define their information management requirements and procedures.

Second, control over funds for managing functional areas has just recently shifted. Now, OSD is to be responsible for managing business decisions and control of these funds no longer remains with the services. Although this change is a significant step in the right direction, service autonomy remains a key barrier.

Third, in what represents a business-as-usual approach, DoD is focusing on selecting specific technology, without concurrently determining what the goal of its C4IFTW system should be and what, if anything, needs to be changed to

bring that vision about. Every service is headed on an individual tangent, hoping to create the C4IFTW system for itself alone. To individually select the technology before making the necessary up-front directional business decisions concerning how information will be managed is like placing the cart before the horse. This out of sequence selection invites risk, creates an illusion of C4IFTW progress, and precludes a substantial portion of CIM's projected thirty-six billion dollar savings. Further, this type of selection is an inefficient way of supporting the warrior, ways that, although automated, will not serve the common goals of tomorrow. The concept of incremental improvement is not at issue. On the contrary, for C4IFTW to survive, incremental business decisions concerning information management must be made before technology is selected.

CONCLUSION

The C4IFTW concept will work. The technologies do exist to make interoperability, global infrastructure, and multi-level security systems realities. The crux of the problem is funding. The C4IFTW concept will be successfully implemented if enough money is dedicated to make it work. With today's budgetary woes, whether the money will be available is in doubt.

Beyond the availability of the money lies the question of service priorities. The money will be spent according

the priorities of the individual services. The value they place on the C4IFTW concept is dependent on whether compliance to C4IFTW standards is tied to acquisition funding. Simply put, if the proposed system does not meet the standards, funding should be denied.

Current doctrine, while well ahead of just one year ago, still does not clearly state that if a service wants to buy a C4I system, the system must be interoperable with the other services, and conform to well defined DoD standards, or it will not be funded. The doctrine does state new systems will be "for joint use," but does not set specific standards. A service may show that the system is available for purchase by the other services, and offer that this fulfills the "for joint use" requirement.

Current approaches to promulgating the C4IFTW concept are on the right track. The "advertising campaign" to convert the service oriented to the joint oriented must continue. All of the "trophies" in the world will not convince some DoD personnel of the dire need for setting aside service agendas in favor the common good. Joint working groups, common testbeds, and shared information are appropriate tools for development of the technology and should be expanded for quicker results.

The Joint Staff has identified the root of the problem as Gen Powell asked them to. It has developed a roadmap for solving the problem. The solution lacks only two key

variables: money and full cooperation of the services. The money may or may not be forthcoming in the future. The DoD has little control over the budgetary future. The cooperation of the services will only come with strict funding control.

Appendix A

13 Standard Data Formats (5)

USE	FORMAT	LONG NAME
Positional	OTG	Over The Horizon Targeting - Gold
	TACREP	Tactical Report
	TACELINT	Tactical ELINT
Fire Support	TACFIRE	Tactical Fire
Intelligence	IDB TF	IDB Transfer Format
Narrative	GENADMIN	General Administration
Flight Operations	ATOCONF	Air Tasking Order Confirmation
Logistics	MILSTRIP	Military Standard Requisitioning and Issue Procedures
	CASREP	Casualty Report
Personnel	SORTSREP	Status of Resources and Training System Report
Force Deployment	ORDER	Order Report
	TPFDD	Time-Phased Force Deployment Data
Force Employment	SITREP	Situation Report

BIBLIOGRAPHY

1. Assistant Secretary of Defense (C3I). Corporate Information Management, Pentagon (OSD). April 1991.

2. Balderman, M., LtCol. "Information Paper, Subject: C4I For The Warrior Update." Pentagon (DISA). 7 Jan 1993.

3. Bryan, D., Col, USA. Executive Summary, C4I for the Warrior, Pentagon (J-6). 8 Jul 1992.

4. C4I Architecture and Integration Division (J-6), The Joint Staff, C4I For the Warrior, Pentagon (J-6). 2 June 1992.

5. C4I Architecture and Integration Division (J-6), The Joint Staff, C4I For The Warrior Interoperability Tiger Team Final Report, Pentagon (J-6). 26 May 1992.

6. C4I Architecture and Integration Division (J-6), The Joint Staff, "Memorandum, Subject: DoD Directive for C4I for the Warrior." Pentagon (J-6). 6 April 1992.

7. Cramer, S., LtCol, USMC. Personal interview, Pentagon (J-6). 28 Jan 1993.

8. Department of Defense. Defense Management Report Decision 918. Pentagon (OSD). 9 Sept 1992.

9. Department of Defense Directive, Number 4630.8, Pentagon (OSD). 12 Nov 1992.

10. Department of Defense Inspector General Memorandum for Assistant Secretary of Defense (C3I). Defense ADP: Corporate Information Management Must Overcome Major Problems. Pentagon (DoDIG). 30 Oct 1992.

11. Department of Defense Instruction, Number 4630.8, Pentagon (OSD). 18 Nov 1992.

12. Defense Information Systems Agency, "DISA Status Briefing on C4I For The Warrior Initiatives." Pentagon (DISA). 14 Jan 1993.

13. Endoso, Joyce. "Joint Chiefs Call for Worldwide Warfighting Network." Government Computing News, 17 Aug 1992:64.

14. Fan, D. Program Specialist, MARCORSYSCOM. Personal Interview. Quantico. 14 Jan 1993.

15. Kurtz, D. Compusec Specialist, MCCTA. Personal Interview. Quantico. 14 Jan 1993.

16. Marine Corps Computer and Telecommunications Activity (MCCTA), CIM and DMRD 918. Quantico. 12 Jan 1993.

17. "Marine Corps Network Security Issues Brief." C4I, HQMC. 2 Oct 1992.

18. Schwartz, Errol. Class lecture. CCSC, COS, MCCDC, Quantico, Virginia. 27 Jan 1993.

19. West, Charles. Target Architecture and Implementation Strategy for the Joint MLS Technology Insertion Program. MLSTIP, DISA. Pentagon (DISA). Sept 1991.